# Detection of Data Exfiltration via Removable Media, Detection Strategy DET0123

Archived: 2026-04-05 14:32:49 UTC

### AN0342

Detects removable drive insertion followed by unusual file access, compression, or staging activity by unauthorized users or unexpected processes.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| DriveTypeFilter | Filter on removable (e.g., USB) drives only. |
| ProcessNameExclusionList | Exclude known, approved backup or sync utilities. |
| TimeWindow | Limit correlation of file access and device mount to a defined window (e.g., <5 minutes). |

### AN0343

Detects mounted external devices (via /media or /mnt) followed by large file read or copy operations by shell scripts, unauthorized users, or staging tools (e.g., tar, rsync).

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| MountPointPattern | Monitor mount points like /media, /mnt, or /run/media. |
| UserGroupScope | Restrict detection to non-root or unexpected users. |
| AccessVolumeThreshold | Alert on large file access or copy events. |

### AN0344

Detects mounting of external volumes followed by high-volume or sensitive file access via Finder, terminal, or third-party apps (e.g., rsync, zip).

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| VolumeNamePattern | Detect suspicious or unrecognized drive labels (e.g., UNTITLED, BACKUP_VOL). |
| ProcessOrigin | Detect CLI-based copy operations vs. expected GUI usage. |
| UserSessionCheck | Alert if process and session context are mismatched (e.g., script from screensaver context). |

---